

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: David J. Allard

Confirmation No.: 9891

Application No. 10/780,098

Examiner: Rangrej, Sheetal

Date filed: February 17, 2004

Group: 3686

For: Method, system, and apparatus for patient controlled access of medical records

---

**REPLY BRIEF UNDER 37 C.F.R. § 41.41**

---

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Arlington, VA 22313-1450

Sir:

This Reply Brief is being filed in response to the Examiner's Answer dated April 13, 2010. Although no fees are believed to be due, the Patent Office is expressly authorized to charge any fees that may be due to Deposit Account No. 14-1437.

**Status of Claims**

Claims 1, 3-4, 16-18, 20, 22-24, and 26-27 are rejected and are being appealed. Claims 2, 5-15, 19, 21, and 25 have been cancelled.

**Grounds of Rejection to be Reviewed on Appeal**

1. Whether claims 1, 3-4, 20, 22-24, and 26-27 are patentable under 35 U.S.C. § 103(a) over U.S. Patent 6,988,075 to Hacker, *et al.* (hereinafter Hacker) in view of non-patent literature, "Public Standards and Patients' Control: How to Keep

Electronic Medical Records Accessible but Private," BMJ, Feb. 2001; 322, pages 283-287 to Mandl, *et al.* (hereinafter Mandl).

2. Whether claims 16-18 are patentable under 35 U.S.C. § 103(a) over Hacker in view of Mandl, and further in view of U.S. Published Patent Application 2002/0010679 to Felsher (hereinafter Felsher).

### **Argument**

It was asserted in the paragraph bridging pages 7 and 8 of the Examiner's Answer that the claim limitations "accessing the medical information by the patient from an access device using a unique patient identifier and a patient PIN" and "assigning each authorized user with a unique authorized user ID and an authorized user PIN" do not differentiate the difference between the patient identifier and an authorized user ID. The claim limitations are broad enough to encompass both the interpretation of the examiner and the Appellant. Hacker teaches providing each patient a unique identification and a passphrase, which is provided to the appropriate medical providers; medical providers access the information using a patient identification and entering the passphrase provided to the medical providers by the patient.

Appellants respectfully disagree. The claim limitations clearly differentiate the difference between the patient identifier and an authorized user ID. In Hacker, a medical provider has to ask a patient for a patient identifier and use the patient identifier to access the information; whereas in the present invention an authorized medical provider is assigned with his or her own unique authorized user ID and can access information using his or her own authorized user ID without asking a patient for a patient identifier.

It was asserted in the second paragraph on page 8 of the Examiner's Answer that Mandl teaches providing the patients the right to decide who can examine and alter what part of their medical records. Mandl further teaches letting the individual control preferences about different aspects of his or her medical history and authorize independently based on the role of the providers.

However, as already discussed in the Appeal Brief, although Mandl mentions that the patient can limit the information to specific providers and provides an override mechanism that is controlled by the patient, Mandl does not suggest using an access control list as the mechanism for controlling access. It is noted that granting different access rights to different providers based on their role is not the same as using an access control list as the mechanism for controlling access. The former is the result and the latter is the mechanism or tool to achieve the result. Mandl does not disclose anywhere using an access control list as the mechanism or tool to achieve granting different access rights to different providers based on their role.

It was asserted in the third paragraph on page 8 of the Examiner's Answer that Hacker teaches notification to the patient as to what information was released to the emergency medical personnel, including time, location, pages accessed, etc. The Examiner stated that Hacker teaches who accessed the medical information by providing the emergency personnel the override and then providing that information to the patient. It was further asserted that Hacker teaches providing information through e-mail pre-authorized by the patient to the medical provider (col. 8, lines 25-40).

However, it is noted that since Hacker does not provide an authorized user, such as a medical provider, with a unique authorized user ID and an authorized user PIN to access the patient information when the patient is not around, the system of Hacker cannot track the identity of the user who accessed the medical information because the emergency medical personnel does not have an authorized user ID. It is noted that the pre-authorized e-mail as disclosed in col. 8, lines 25-40 of Hacker is based on patient ID, not on an authorized user ID, and thus also does not track the identity of the medical provider who accessed the information.

Regarding claims 3, 22, and 26, it is noted that unique access identification means is not necessarily a universally unique identifier in the sense of the present invention. Unique access identification means could only be unique to a particular record system, such as in current hospital system, but not unique to other record systems, such as in other hospital systems.

Regarding claim 4, 23, and 27, Hacker proposes an override for emergency situations but does not teach the mechanism of registration of emergency providers. Preventing the access to information by those searching for private information and posing to be an emergency provider is the advantage that can be achieved by the claimed invention and does not have to be recited in the claims.

Regarding claim 17, it is noted that in Felsher the system determines the length of the session (such as 15 minutes) whereas in the present invention the patient controls the length of the session.

Regarding claims 18, Felsher does not disclose that access to the patient's medical information expires when a physician logs into another room/appointment. Verification of the user for access after the time limit parameters is not the same as access to the patient's medical information expires when a physician logs into another room/appointment. The time limit parameters can expire even without the physician logging into another room/appointment. Conversely, a physician can log into another room/appointment to cause access to the patient's medical information to expire even if the time limit parameters do not expire.

In view of the forgoing as well as the arguments in the Appeal Brief, the honorable Board is therefore respectfully urged to reverse the final rejection of the Primary Examiner.

Respectfully submitted,

NOVAK DRUCE + QUIGG LLP

Date: **June 14, 2010**

/Gregory A. Nelson/

Gregory A. Nelson, Registration No. 30,577

Yonghong Chen, Registration No. 56,150

525 Okeechobee Blvd., 15<sup>th</sup> Floor

West Palm Beach, FL 33401

Telephone: (561) 847-7800